

CLAIMS

- 1 1. A method for secure key delivery for decrypting a distribution archive file at an
2 unsecure site that receives a stream of distribution archive files from a publishing
3 site, the method comprising:
 - 4 (a) extracting a scheduled key from a first distribution archive file in the
5 stream;
 - 6 (b) using the retrieved scheduled key to decrypt the next distribution archive
7 file in the stream following the first distribution archive file; and
 - 8 (c) repeating steps (a) and (b) for each distribution archive file in the stream.
- 1 2. The method of claim 1 further comprising:
 - 2 (d) receiving a scheduled key for the first distribution archive file in the stream
3 from the publishing site.
- 1 3. The method of claim 1 wherein each distribution archive file comprises a plurality
2 of encrypted content files and wherein the method further comprises:
 - 3 (d) encrypting, with a scheduled key, a distribution archive file including a
4 scheduled key for the next distribution archive file in the stream and the
5 plurality of encrypted content files.
- 1 4. The method of claim 1 wherein each distribution archive file comprises a plurality
2 of encrypted content files and wherein the method further comprises:
 - 3 (d) encrypting, with a scheduled key, a distribution archive file including the
4 plurality of encrypted content files and a non-encrypted scheduled key for
5 the next distribution archive file.
- 1 5. The method of claim 1 wherein each distribution archive file comprises a plurality
2 of digital content documents and the method further comprises:

- 3 (d) at the publishing site, encrypting each digital content document with a key
- 4 to generate encrypted document content;
- 5 (e) at the publishing site, computing for each document, from the encrypted
- 6 document content for that document, a document identifier that cannot be
- 7 derived solely from the encrypted version of the requested document;
- 8 (f) at the publishing site, creating a list of document identifier and decryption
- 9 key pairs;
- 10 (g) at the publishing site, assembling the encrypted document content for
- 11 each content document and the key pair list into a distribution archive file;
- 12 and
- 13 (e) encrypting the distribution archive file with a scheduled key.

1 6. The method of claim 5 wherein step (g) comprises generating a new scheduled
2 key, encrypting the new scheduled key and including the encrypted scheduled
3 key in the distribution archive file.

1 7. The method of claim 6 wherein the new scheduled key is encrypted using a text
2 string embedded in program code in the publishing site.

1 8. The method of claim 7 wherein step (a) comprises storing an extracted
2 scheduled key in encrypted form.

1 9. The method of claim 8 wherein the extracted scheduled key is encrypted with a
2 text string embedded in program code at the unsecure site.

1 10. The method of claim 9 wherein the text string embedded in program code in the
2 publishing site is the same as the text string embedded in program code at the
3 unsecure site.

- 1 11. Apparatus for secure key delivery for decrypting a distribution archive file at an
2 unsecure site that receives a stream of distribution archive files from a publishing
3 site, the apparatus comprising:
4 a key decryptor that extracts a scheduled key from each distribution
5 archive file in the stream;
6 means for temporarily storing the extracted scheduled key; and
7 a decryption engine that uses the stored scheduled key to decrypt the next
8 distribution archive file in the stream following the distribution archive file from
9 which the scheduled key was extracted.
- 1 12. The apparatus of claim 11 further comprising means for receiving a scheduled
2 key for the first distribution archive file in the stream from the publishing site.
- 1 13. The apparatus of claim 11 wherein each distribution archive file comprises a
2 plurality of encrypted content files and wherein the apparatus further comprises
3 an encryption engine that encrypts, with a scheduled key, a distribution archive
4 file including a scheduled key for the next distribution archive file in the stream
5 and the plurality of encrypted content files.
- 1 14. The apparatus of claim 11 wherein each distribution archive file comprises a
2 plurality of encrypted content files and wherein the apparatus further comprises
3 an encryption engine that encrypts, with a scheduled key, a distribution archive
4 file including the plurality of encrypted content files and a non-encrypted
5 scheduled key for the next distribution archive file.
- 1 15. The apparatus of claim 11 wherein each distribution archive file comprises a
2 plurality of digital content documents and the apparatus further comprises:
3 at the publishing site, an encryption engine that encrypts each digital
4 content document with a key to generate encrypted document content;

5 at the publishing site, an OID calculator that computes for each document,
6 from the encrypted document content for that document, a document identifier
7 that cannot be derived solely from the encrypted version of the requested
8 document;

9 at the publishing site, means for creating a list of document identifier and
10 decryption key pairs;

11 at the publishing site, means for assembling the encrypted document
12 content for each content document and the key pair list into a distribution archive;
13 and

14 means for encrypting the distribution archive with a scheduled key.

1 16. The apparatus of claim 15 wherein the means for encrypting the distribution
2 archive with a scheduled key comprises a key generator that generates a new
3 scheduled key, a key encryptor that encrypts the new scheduled key and means
4 for including the encrypted scheduled key in the distribution archive.

1 17. The apparatus of claim 16 wherein the key encryptor encrypts the new scheduled
2 key using a text string embedded in program code in the publishing site.

1 18. The apparatus of claim 17 wherein the means for temporarily storing the
2 extracted scheduled key comprises means for storing an extracted scheduled
3 key in encrypted form.

1 19. The apparatus of claim 18 wherein the means for temporarily storing the
2 extracted scheduled key comprises means for encrypting the extracted
3 scheduled key with a text string embedded in program code at the unsecure site.

1 20. The apparatus of claim 19 wherein the text string embedded in program code in
2 the publishing site is the same as the text string embedded in program code at
3 the unsecure site.

- 1 21. A computer program product for secure key delivery for decrypting a distribution
2 archive file at an unsecure site that receives a stream of distribution archive files
3 from a publishing site, the computer program product comprising a computer
4 usable medium having computer readable program code thereon, including:
5 program code for extracting a scheduled key from each distribution
6 archive file in the stream;
7 program code for temporarily storing the extracted scheduled key; and
8 program code for using the stored scheduled key to decrypt the next
9 distribution archive file in the stream following the distribution archive file from
10 which the scheduled key was extracted.
- 1 22. The computer program product of claim 21 further comprising program code for
2 receiving a scheduled key for the first distribution archive file in the stream from
3 the publishing site.
- 1 23. The computer program product of claim 21 wherein each distribution archive file
2 comprises a plurality of encrypted content files and wherein the computer
3 program product further comprises:
4 program code for encrypting, with a scheduled key, a distribution archive
5 file including a scheduled key for the next distribution archive file in the stream
6 and the plurality of encrypted content files.
- 1 24. The computer program product of claim 21 wherein each distribution archive file
2 comprises a plurality of encrypted content files and wherein the computer
3 program product further comprises:
4 program code for encrypting, with a scheduled key, a distribution archive
5 file including the plurality of encrypted content files and a non-encrypted
6 scheduled key for the next distribution archive file.

1 25. The computer program product of claim 21 wherein each distribution archive file
2 comprises a plurality of digital content documents and the method further
3 comprises:

4 program code at the publishing site, for encrypting each digital content
5 document with a key to generate encrypted document content;

6 program code at the publishing site, for computing for each document,
7 from the encrypted document content for that document, a document identifier
8 that cannot be derived solely from the encrypted version of the requested
9 document;

10 program code at the publishing site, for creating a list of document
11 identifier and decryption key pairs;

12 program code at the publishing site, for assembling the encrypted
13 document content for each content document and the key pair list into a
14 distribution archive file; and

15 program code for encrypting the distribution archive file with a scheduled
16 key.

1 26. The computer program product of claim 25 wherein the program code for
2 encrypting the distribution archive file comprises program code for generating a
3 new scheduled key, program code for encrypting the new scheduled key and
4 program code for including the encrypted scheduled key in the distribution
5 archive file.

1 27. The computer program product of claim 26 wherein the program code for
2 encrypting the new scheduled key encrypts the new scheduled key using a text
3 string embedded in program code in the publishing site.

1 28. The computer program product of claim 27 wherein the program code for
2 temporarily storing the extracted scheduled key comprises program code for
3 storing an extracted scheduled key in encrypted form.

- 1 29. The computer program product of claim 28 wherein the program code for
2 encrypting the extracted scheduled key encrypts the extracted scheduled key
3 with a text string embedded in program code at the unsecure site.
- 1 30. The computer program product of claim 29 wherein the text string embedded in
2 program code in the publishing site is the same as the text string embedded in
3 program code at the unsecure site.